CONTINUATION OF APPLICATION FOR A SEARCH WARRANT

1. I, Rodney M. Charles, Special Agent (SA) of the Federal Bureau of Investigation (FBI), Lansing, Michigan, United States Department of Justice, have been employed as an SA of the FBI for almost 23 years. During my employment with the FBI, I have conducted investigations into a variety of federal criminal laws, and I have significant experience in enforcement of those laws. I have also supervised, investigated, and assisted other agents in child exploitation and child pornography investigations, which included violations pertaining to the distribution, receipt, or possession of child pornography, in violation of 18 U.S.C. §2252A. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

INTRODUCTION AND PURPOSE OF THE WARRANT

2. I make this continuation in support of an application for a search warrant to search **3705 Maybel Street, Lansing, Michigan** (the "SUBJECT PREMISES"), for evidence, contraband, fruits, and instrumentalities of crime in violation of 18 U.S.C. §§ 2252A(a)(2) (distribution or receipt of child pornography) and 2252A(a)(5)(B) (possession of child pornography). These items are more specifically described in Attachment B.

3. This investigation has revealed that there is likely a computer device or devices with an internet connection located at **3705 Maybel Street, Lansing, Michigan**, that has been used to receive, store, and distribute child pornography.

4. As set forth herein, probable cause exists to believe there have been violations of 18 U.S.C. § 2252A originating from **3705 Maybel Street, Lansing, Michigan**, and that evidence, contraband, fruits, and instrumentalities of crime are likely to be found at that location. The search contemplated by this continuation will include the residence; outbuildings within the curtilage; any vehicles present at the time of the execution of the search warrant that are owned or controlled by any residents of the premises whether those residents are present or not; persons who reside at the residence who are present at the time the search warrant is executed, and a search of any computer, digital, and related media located therein, for items specified in Attachment B.

5. The search of the vehicles is to include all internal and external compartments and all containers that may be associated with the storage of child pornographic materials or their instrumentalities contained within the aforementioned vehicles and adjacent structures. The search of the residents present on the property is to locate any digital storage devices on their person that may contain evidence of child pornography, or passwords or other information necessary to access evidence of child pornography found elsewhere.

6. The items to be searched for and seized, more specifically detailed in Attachment B, include computers, computer media, external data storage devices, smartphones, tablets, digital media players, and hard copy media such as magazines and photographs.

7. I am familiar with the information contained in this continuation

based upon the investigation I have conducted, and based on information provided to me by other law enforcement officers who have engaged in investigations involving the distribution of child pornography.

8. The facts in this continuation come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this continuation is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities in violation of 18 U.S.C. § 2252A are presently located at or in **3705 Maybel Street, Lansing, Michigan.**

RELEVANT STATUTES

9. This investigation concerns alleged violations of 18 U.S.C. § 2252A:

a. Section 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed, or using any means or facility or interstate commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or knowingly receiving or distributing any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. Section 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

10. Pursuant to the provisions of 18 U.S.C. § 2256, "child pornography" means a visual depiction, the production of which involves the use of a minor engaging in sexually explicit conduct, including but not limited to various simulated or actual sex acts, or the lascivious exhibition of the genitals or pubic area.

PEER-TO-PEER FILE-SHARING NETWORKS

11. "Peer-to-peer file-sharing" (P2P) is a method of communication available to Internet users through the use of special software. Computers link together through the Internet using this software, which allows direct sharing of digital files between users on the same network. A user first obtains the P2P software, which can be downloaded from the Internet. A user obtains files by opening the P2P software on the user's computer and conducting searches for files that are currently being shared on other users' computers.

12. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. The numerical IP address is unique to a particular computer during an online session. The IP address identifies the physical location of the computer with which the address is associated. Third-party software is available to identify the IP address of the P2P computer sending the file.

13. The BitTorrent network is a very popular and publically available P2P file-sharing network. A user can download files from other users simultaneously and provide files to others.

14. Undercover law enforcement officers can setup a BitTorrent account to search for and download files from other users. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between an investigator's BitTorrent client program and the suspect client program. This information includes (1) the suspect client's IP address; (2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and (3) the BitTorrent network client program and version being used by the suspect computer.

15. Law enforcement can locate files available on the BitTorrent network by searching for certain keywords and/or by searching for known files of investigative interest that have previously been identified as child pornography. Child pornography files that have previously been discovered in other investigations are catalogued in a national database, and each image has a unique "hash" value

that is like a digital fingerprint. Investigators can detect whether known files of investigative interest are being shared on a P2P network by searching for and downloading files with those hash values.

FACTUAL BACKGROUND OF INVESTIGATION

16. On May 27, 2015, SA Raymond C. Nichols from the Detroit Division of the FBI was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Nichols directed his investigative focus to a device at IP address **76.20.151.234** because it was associated with a torrent with a known hash value. SA Nichols knew this hash value contained child pornography based on previous investigations.

17. Using a computer running investigative BitTorrent software, SA Nichols directly connected to the device at IP address **76.20.151.234**, hereinafter referred to as the "suspect device." The suspect device reported it was using BitTorrent client software BT7930-BitTorrent 7.9.3.

18. On Wednesday, May 27, 2015, between 1932 hours and 2218 hours, SA Nichols successfully completed the download of approximately 40 files that the suspect device at IP address **76.20.151.234** was making available. The device at IP address **76.20.151.234** was the sole candidate for each download, and as such, each file was downloaded directly from this IP address.

19. The above referenced files were reviewed by SA Nichols and many appeared to meet the federal definition of child pornography. SA Nichols also provided the files to me. These approximately 40 files include minor male and

female children in various states of undress. The images also depict oral, vaginal and anal penetration. Among the images, there are also several National Center for Missing and Exploited Children "known" database series images. Examples of some of the images are: an image of a nude prepubescent female engaged in oral sex with an adult male; an image of adult male genitals touching the exterior of prepubescent female genitals; several images of adult male genitals penetrating prepubescent female genitals.

20. On Thursday, May 28, 2015, SA Nichols conducted a query on the IP Address **76.20.151.234** and found it was registered to Comcast Cable Communications, Inc.

21. On May 29, 2015, in response to an administrative subpoena, Comcast provided subscriber information for the referenced IP address **76.20.151.234** as:

Name: Joshua Micka

Address: **3705 Maybel Road**

Lansing, Michigan 48911

Telephone: (989) 640-0446

E-Mail: jmicka@comcast.net

22. Upon receiving this lead, for several months, the FBI attempted to confirm that Joshua Micka resided at **3705 Maybel Street, Lansing, Michigan**. The majority of instances where agents surveilled **3705 Maybel Street**, there were no vehicles in the driveway. When there was a vehicle present, agents never observed anyone leaving the residence or entering the vehicle. Then, on January

20, 2017, SA Patrick Kelly was watching **3705 Maybel Street, Lansing, Michigan** and observed a vehicle parked in the driveway. The vehicle was registered to Cheryl Micka, who is believed to be Joshua Micka's mother, per open source information. Eventually, SA Kelly saw a white man exit the front door, enter the vehicle, and drive away. The man was wearing a hooded sweatshirt with the hood up, so SA Kelly could not confirm the male was Micka. Several minutes later, the vehicle was stopped by an officer from the Lansing Township Police Department. The driver was then identified as Joshua John Micka. This was the first time the FBI could confirm Micka was located at **3705 Maybel Street, Lansing, Michigan**.

23. A subpoena was issued on December 12, 2016, to Comcast for subscriber and IP history records pertaining to Joshua Micka with SSN 372-98-2839 at address **3705 Maybel Road, Lansing, MI 48911,** with service from November 22, 2016, to December 12, 2016. On December 16, 2016, Comcast provided records for the requested timeframe, and the account information was the same (i.e., the residential address and registered user were Joshua Micka at **3705 Mabel Road, Lansing MI 48911**). However, the records disclosed the Comcast account number for this subscriber changed from 0172121189703 (Old Account Number) to 8529113980619270 (New Account Number). IP history records provided for this timeframe showed IP address **24.127.117.226** was assigned to account number 8529113980619270 from June 19, 2016, to December 08, 2016.

24. Using a law enforcement sensitive database on January 11, 2018, the

FBI was able to determine that on 11/27/2016, IP address **24.127.117.226** was sharing files on the BitTorrent network. The IP address **24.127.117.226** was associated with a torrent that contained approximately 681 files. Based on the hash values of the files, some of these files have been identified to contain child pornography by other investigators. Some files are known to be of a seven year old female exposing her genitals and modeling unclothed.[1]

25. On January 10, 2018, I conducted at knock and talk at **3705 Mabel Lansing, MI** with SA Kelly. At that time, Micka was home; Micka asked for clarification on why we wanted to talk to him. We said we were following up on a lead that his computer may have a virus or may have been hacked into, and we were there to inquire whether he would grant permission for an FBI computer expert to look at his computer. Micka advised he'd prefer to not have the FBI look at his computer and instead take it to someone else himself. Micka admitted he has lived at this house for approximately five to six years. He had roommates about four or five years ago but has lived by himself since then. One of the roommates had a laptop at that time. Micka has had two computers of his own while living at this address. The hard drive in his older computer froze up and became inoperable, so he purchased a new computer sometime in 2016 or early 2017. Micka claimed he did not copy the files from his old computer, as it froze up, and he threw this old

[1] "As a preliminary matter, stale information cannot be used in a probable cause determination … Thus, the court must first focus on whether information that is sixteen-months old is stale …. With respect to images of child pornography, however, the answer may be no because the images can have an infinite life span." *United States v. Frechette,* 583 F.3d 374, 378 (6th Cir. 2009) (internal citations omitted).

computer away. Micka advised he was not a computer expert, and he just plays games on his computer.

26. Based on the investigation and Micka's admissions, I know that as of January 10, 2018, there is a modem and at least one computer in his home. I know from my training and experience that modems will maintain a log of what devices were accessing the internet through that modem. Therefore, the modem may provide information about what devices were being used to distribute child pornography from the IP addresses associated with **3705 Maybel Street Lansing, Michigan**.

27. The activity from the IP addresses that resolved to **3705 Maybel Street Lansing, Michigan** in 2015 and 2016 is consistent with an individual who is a consumer and collector of child pornography material. According to the Micka's admissions, he was residing at **3705 Maybel Street Lansing, Michigan** the entire time that such activity occurred. To the extent that Micka claimed he had a roommate "four or five years ago," at most, the roommate was present when child pornography was being shared in 2015, but would not have still been present in 2016. Therefore, I believe there is probable cause to believe that Micka is a consumer and collector of child pornography, i.e. a person with a sexual interest in children.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

28. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience

of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the distribution, receipt, and collection of child pornography. There is probable cause to believe that a person using the internet at **3705 Maybel Street, Lansing, Michigan** is a collector of child pornography based on the large number of files being shared on the P2P network. Characteristics common to people involved in Internet child pornography include that they:

a. Generally have a sexual interest in children and receive sexual gratification viewing children engaged in sexual activity or in sexually suggestive poses, or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including in hard copy and/or digital formats. Child pornography viewers and collectors oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse or groom a child to participate in sex, or to demonstrate the desired sexual acts. They may also use toys, games, costumes, sexual clothing, sexual paraphernalia, and children's clothing to lure or entice children. They may keep "trophies" or mementos of sexual encounters with children, or items that they use to gratify a sexual interest in children, such as by collecting children's underwear or other items belonging to a child.

c. May take photographs that either constitute child pornography or indicate a sexual interest in children by using cameras, video cameras, web cameras, and cellular telephones. Such images and video may be taken with or without the child's knowledge. This type of material may be used by the person to gratify a sexual interest in children.

d. Generally maintain their collections in a safe, secure, and private environment, most often where they live and/or on their person. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images can be stored in both digital and hard copy format and are usually hidden so that they are not found by other members of the residence or by anyone else who enters the home. Such hiding places could include but are not limited to garages, sheds, attics, vehicles, bags, and pockets. Digital files and devices may be password protected, encrypted, or otherwise protected.

e. May correspond with and/or meet others to share information

and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Such correspondence may take place, for example, through online bulletin boards and forums, Internet-based chat messaging, email, text message, video streaming, letters, telephone, and in person.

29. There is probable cause to believe that an individual using the internet service registered to address **3705 Maybel Street, Lansing, Michigan**, is a child pornography collector using the BitTorrent network, a P2P network, to trade child pornography. Such activity is indicative that a user of the Internet service registered to address **3705 Maybel Street, Lansing, Michigan**, fits the characteristics of a collector of child pornography.

SPECIFICS OF SEIZING AND SEARCHING COMPUTER SYSTEMS

30. Computers and internet-capable devices such as tablets and cellular telephones facilitate the collection and distribution of child pornography. The internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

31. Storage capacity of computers and portable storage media, such as

USB or thumb drives, has grown tremendously within the last several years. These drives can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or in any number of easily transportable and concealable places. An individual can now easily carry on his or her person storage media that contains thousands of files, including images, video files, and full-length movie files.

32. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer user's internet activities generally leave traces in a computer's web cache and internet history files.

33. A forensic examiner often can recover evidence that shows whether a computer device contains peer-to-peer software, when the device was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the internet. Electronic files

downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that date remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

34. Similarly, files that have been viewed via the internet are automatically downloaded into a temporary internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

35. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

36. In order to retrieve data fully from a computer system, the analyst

needs all storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

37. To examine the computer and digital media properly, it may also be necessary to seize certain other items including documentation of programs, passwords, notes, or even specialized hardware. Therefore, this warrant seeks permission to seize not only the digital storage media and to search it for evidence in the form of child pornography images or videos, stored emails associated with the receipt and distribution of such images, and any chat or other text files relating to contact with collectors of child pornography or with actual children, but also requests permission to seize all hardware, software, and computer security devices necessary to access and examine the computer storage media. Peripheral equipment including printers, routers, modems, network equipment used to connect to the internet may also contain evidence of what devices were used to connect to the internet, who used those devices, and what actions the person(s) performed while using such devices.

38. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer at a given time.

Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop-up blockers, security software, password protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain. The Government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

39. Items determined on-scene not to contain items listed in Attachment B will be left at the SUBJECT PREMISES. The remaining items will be seized and searched for further review or forensic examination and will be returned as soon as reasonably possible if they are determined not to contain evidence listed in Attachment B.

40. Retention of any computers would be warranted, if any child pornography is found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to 18 U.S.C. §§ 2253(a)(3) and 2254(a)(2).

REQUEST FOR SEALING

41. I respectfully request that the Court issue an order sealing, until further order of this Court, all papers submitted in support of this application, including the application, continuation, attachments, and search warrant, and the requisite inventory notice. I believe sealing is necessary because premature disclosure of the contents of this continuation and related documents may jeopardize this continuing investigation by alerting the target(s) and providing an opportunity to destroy evidence.

CONCLUSION

42. I respectfully submit that there is probable cause to believe that an individual who resides at **3705 Maybel Street, Lansing, Michigan**, is involved in the receipt, distribution, and possession of child pornography and has violated 18 U.S.C. § 2252A(a)(2) and (a)(5)(B), and that evidence, fruits, and instrumentalities of those crimes, listed in Attachment B are located in the residence.

43. Wherefore, by this continuation and application, I respectfully request that the Court issue a search warrant that would allow agents to search for and seize evidence from **3705 Maybel Street, Lansing, Michigan**. The items and information sought to be seized are more specifically described in Attachment B.